realm of possibility, but because of a vision and because of a commitment and a desire to push the bounds of our capabilities, they persevered and we found a way. MD Anderson's Moon Shots Program serves as another example of American ingenuity, ambition, and dogged determination to make the lives of our families and the future generations better than our own.

Fortunately, as I said, this Cures bill the House will be voting on today, which we will vote on next week, will provide funding for cancer and Alzheimer's research, among other terrible diseases, so that the best medical community in the world can help make great strides in fighting them.

This legislation will also fund the battle against opioid abuse, prescription drug abuse—something we have discussed a lot here on the floor during the last year because of the devastation that it has brought about in many parts of the country. Of course, we know that when the opioids aren't available, cheap heroin imported into the United States from south of our border is part of that scourge as well.

Overdoses and the abuse of opioid drugs are tearing families apart. This bill will provide additional grant funding to States to combat it and to help people who are already in the grips of this terrible addiction to find a way to freedom.

I am particularly glad that this legislation includes bipartisan mental health reforms that I introduced in this Chamber last year, known as the Mental Health and Safe Communities Act. I want to express my gratitude to Senator ALEXANDER, Senator MURRAY, and others on a bipartisan basis and bicameral basis for working with us to make sure we include mental health reform as a component of the 21st Century Cures legislation.

We all know that mental health problems are something that American families have to deal with. I dare say there is probably not a family in America that doesn't have to deal with this in some way or another—either at work, with people you go to church with, or with people you live next door to. In some way or another, mental health problems are rampant.

A lot of that has to do with well-intended but unintended consequences of deinstitutionalization of our mentally ill back in the 1990s. The idea was that it was not appropriate to institutionalize people with mental illness, and so we ought to deinstitutionalize them. But we contemplated that there would be some sort of safety net after they went back to their communities where they could get treatment and where they would get the care they needed. Unfortunately, what has happened and what my legislation is designed to address is that our jails have become the de facto default mental health treatment facilities in this country.

I recently was at a meeting of a large county sheriffs association in Washington, DC, and a friend of mine, the current sheriff of Bexar County, TX, Sheriff Pamerleau, said: How would you like to meet the largest mental health provider in America? I said: Well, sure.

She walked across the floor and introduced me to the sheriff of Los Angeles County, who runs the Los Angeles County jails. You get my point. We are warehousing people in jails and other places and not giving them the treatment they need in order to get their basic underlying problem taken care of. Of course, people with untreated mental illness frequently engage in petty crimes—trespassing and other things—which end them up in jail. But if they don't get treated, they are going to stay in that turnstile and keep coming back.

We all know the problem of homelessness in our streets. You walk down the street in Washington, DC, or any city in the country—such as Austin, TX—and you see people who have obvious symptoms of mental illness who are not being treated. What this legislation does is to provide a pathway to treatment, primarily by using preexisting appropriations to make grants to our States and local communities so they can deal with these using the very best practices in the country. For example, the Federal Government already spends about $2 billion a year on grants to State and local law enforcement. Doesn't it make sense to prioritize dealing with these mental health problems and particularly with the best practices in places such as San Antonio, TX, where the mental health community and law enforcement and other leaders have come together to try to come up with a program to divert people with mental illness to treatment and to provide additional training to law enforcement, to deescalate some of the conflicts that occur—for example, when the police show up and confront somebody with obvious mental illness. If the police don't get the kind of training they need, then that could end up in a tragedy, either for the person being arrested or for the police officers.

It is really important that we deal with this in a sensible way, and this legislation helps to do that—again, using some of that $2 billion in grant funding we give to State and local law enforcement but prioritizing and authorizing some of the very best practices occurring in communities around the country so that more people can benefit from these programs.

This also provides families additional tools. For example, if you have a family member who is suffering from severe mental illness—let's say they are an adult—there is not a whole lot you can do about it if they refuse to seek treatment or comply with their doctor's orders. There is a means—a very difficult means—for temporary institutionalization. For example, you have to get a doctor's order and then go to court and get somebody put in a State hospital or an institution, but they are not there forever. They may be there for 30 days or so, until their symptoms abate because they are complying with their doctor's orders and taking their medication.

The great news in mental health treatment is there are a lot of miraculous treatments, and if the person afflicted with mental illness will comply with their doctor's orders and take their medication, they can lead relatively normal and productive lives. But the great problem is that so often people refuse to take their medication. They start feeling better. They quit, and they become sicker and sicker, until they become a danger both to themselves and the community.

One of the things this legislation does is to provide an additional procedure, called assisted outpatient treatment, which gives local courts and civil courts the authority to consider a petition whereby a family member can come in and say: My son, my daughter, my husband, my relative is having serious problems with their mental illness and they are noncompliant with their treatments. Judge, will you please enter an order, which essentially is like probation, saying that periodically you have to come back and report to the court on your compliance with the order, but part of that is to follow your doctor's orders and to take your medication. I am not saying it is a panacea, but it provides family members another tool when their loved ones become mentally ill and when there are no good options for the family members to assure that they will get the treatment or remain compliant with their doctor's orders by taking their medication.

I applaud the House for taking up these critical reforms. I know Congressman TIM MURPHY has worked on this long and hard in the House. There are a lot of other people who have worked on this mental health reform. In this Chamber, Senator BILL CASSIDY has been a champion and CHRIS MURPHY, among others. Really, the persons who have gotten us this far—there are two of them—are Senator ALEXANDER and Senator MURRAY, the chairman and the ranking member of the HELP Committee. But it has taken a bipartisan, bicameral effort to try to get us to this point, and I am glad that we will be voting on this next week, after the House passes it today.

With that, I yield the floor.

The PRESIDING OFFICER (Mr. SULLIVAN). The Senator from Oregon.

UNANIMOUS CONSENT REQUEST—S. 2952

Mr. WYDEN. Mr. President, absent Senate action, at midnight tonight, this Senate will make one of the biggest mistakes in surveillance policy in years and years. Without a single congressional hearing, without a shred of meaningful public input, without any opportunity for Senators to ask their

questions in a public forum, one judge with one warrant would be able to authorize the hacking of thousands—possibly millions—of devices, cell phones, and tablets. This would come about through the adoption of an obscure rule of criminal procedure called rule 41. Rule 41 isn't something folks are talking about in coffee shops in Alaska, in Oregon, and in other parts of the country, but I am convinced Americans are sure going to come to Members of Congress if one of their hospitals—one of their crucial medical programs—is hacked by the government. It is a fact that one of the highest profile victims of cyber attacks are medical facilities, our hospitals.

The Justice Department has said this is no big deal. You basically ought to trust us. We are just going to take care of this. I will tell you, generally, changes to the Federal rules of procedure are designed for modest, almost housekeeping kinds of procedural changes, not major shifts in policies. When you are talking about these kinds of rules, they talk about who might receive a copy of a document in a bankruptcy proceeding. That is what the Rules Enabling Act was for. It wasn't for something that was sweeping, that was unprecedented, that could have calamitous ramifications for Americans the way government hacking would. As I have indicated, this would go forward without a chance for any Member of the Senate to formally weigh in.

The government says it can go forward with this rule 41 and conduct these massive hacks—large-scale hacks—without causing any collateral damage whatsoever and ensuring that Americans' rights are protected. Oddly enough—again, breaking with the way these matters are usually handled—the government will not tell the Congress or the American people how it would protect those rights or how it would prevent collateral damage or even how it would carry out these hacks. In effect, the policy is ''trust us.''

I think that right at the heart of our obligations is to do vigorous oversight. I always thought Ronald Reagan had a valid point when he said: You can trust but you ought to verify. That is especially important under this policy, where innocent Americans could be victimized twice—once by their hackers and a second time by their government.

We are going to have the opportunity to do something about it before this goes into effect in just over 12 hours. I want to emphasize that those of us who would like the chance for Members of Congress to weigh in and be heard—our concern has been bipartisan. Senator COONS. Senator DAINES. We have worked in a bipartisan fashion on this for months.

This morning we are going to offer three unanimous consent requests to block or delay this particular change in order to make sure our colleagues have an opportunity to do what I think is Senate 101: to have a hearing and have a review that is bipartisan, where Senators get to ask questions, to be able to get public input in a meaningful kind of fashion.

I urge every Senator to think, and think carefully, before they prevent this body from performing the vigorous oversight Americans demand of Congress. That is right at the heart of what Senator COONS, Senator DAINES, and I will be talking about. This rule change will give the government unprecedented authority to hack into Americans' personal phones, computers, and other devices. Frankly, I was concerned about this before the election, but we now know that the administration—it is a new administration—will be led by the individual who said he wanted the power to hack his political opponents the same way Russia does. These mass hacks could affect cell phones, desktop computers, traffic lights, not to mention a whole host of different areas. During these hacks and searches, there is a considerable chance that the hacked devices will be damaged or broken, and that would obviously be a significant matter. Don't take my word for it.

Mr. President, I ask unanimous consent to have an article that I wrote with renowned security experts Matt Blaze and Susan Landau printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

[From Wired.com, Sept. 14, 2016]

THE FEDS WILL SOON BE ABLE TO LEGALLY HACK ALMOST ANYONE

(By Senator Ron Wyden, Matt Blaze and Susan Landau)

Digital devices and software programs are complicated. Behind the pointing and clicking on screen are thousands of processes and routines that make everything work. So when malicious software—malware—invades a system, even seemingly small changes to the system can have unpredictable impacts.

That's why it's so concerning that the Justice Department is planning a vast expansion of government hacking. Under a new set of rules, the FBI would have the authority to secretly use malware to hack into thousands or hundreds of thousands of computers that belong to innocent third parties and even crime victims. The unintended consequences could be staggering.

The new plan to drastically expand the government's hacking and surveillance authorities is known formally as amendments to Rule 41 of the Federal Rules of Criminal Procedure, and the proposal would allow the government to hack a million computers or more with a single warrant. If Congress doesn't pass legislation blocking this proposal, the new rules go into effect on December 1. With just six work weeks remaining on the Senate schedule and a long Congressional to-do list, time is running out.

The government says it needs this power to investigate a network of devices infected with malware and controlled by a criminal—what's known as a ''botnet.'' But the Justice Department has given the public far too little information about its hacking tools and how it plans to use them. And the amendments to Rule 41 are woefully short on protections for the security of hospitals, life-saving computer systems, or the phones and electronic devices of innocent Americans.

Without rigorous and periodic evaluation of hacking software by independent experts, it would be nothing short of reckless to allow this massive expansion of government hacking.

If malware crashes your personal computer or phone, it can mean a loss of photos, documents and records—a major inconvenience. But if a hospital's computer system or other critical infrastructure crashes, it puts lives at risk. Surgical directives are lost. Medical histories are inaccessible. Patients can wait hours for care. If critical information isn't available to doctors, people could die. Without new safeguards on the government's hacking authority, the FBI could very well be responsible for this kind of tragedy in the future.

No one believes the government is setting out to damage victims' computers. But history shows just how hard it is to get hacking tools right. Indeed, recent experience shows that tools developed by law enforcement have actually been co-opted and used by criminals and miscreants. For example, the FBI digital wiretapping tool Carnivore, later renamed DCS 3000, had weaknesses (which were eventually publicly identified) that made it vulnerable to spoofing by unauthorized parties, allowing criminals to hijack legitimate government searches. Cisco's Law Enforcement access standards, the guidelines for allowing government wiretaps through Cisco's routers, had similar weaknesses that security researchers discovered.

The government will likely argue that its tools for going after large botnets have yet to cause the kind of unintended damage we describe. But it is impossible to verify that claim without more transparency from the agencies about their operations. Even if the claim is true, today's botnets are simple, and their commands can easily be found online. So even if the FBI's investigative techniques are effective today, in the future that might not be the case. Damage to devices or files can happen when a software program searches and finds pieces of the botnet hidden on a victim's computer. Indeed, damage happens even when changes are straightforward: recently an anti-virus scan shut down a device in the middle of heart surgery.

Compounding the problem is that the FBI keeps its hacking techniques shrouded in secrecy. The FBI's statements to date do not inspire confidence that it will take the necessary precautions to test malware before deploying them in the field. One FBI special agent recently testified that a tool was safe because he tested it on his home computer, and it ''did not make any changes to the security settings on my computer.'' This obviously falls far short of the testing needed to vet a complicated hacking tool that could be unleashed on millions of devices.

Why would Congress approve such a short-sighted proposal? It didn't. Congress had no role in writing or approving these changes, which were developed by the US court system through an obscure procedural process. This process was intended for updating minor procedural rules, not for making major policy decisions.

This kind of vast expansion of government mass hacking and surveillance is clearly a policy decision. This is a job for Congress, not a little-known court process.

If Congress had to pass a bill to enact these changes, it almost surely would not pass as written. The Justice Department may need new authorities to identify and search anonymous computers linked to digital crimes. But this package of changes is far too broad, with far too little oversight or protections against collateral damage.

Congress should block these rule changes from going into effect by passing the bipartisan, bicameral Stopping Mass Hacking Act.

Americans deserve a real debate about the best way to update our laws to address online threats.

Mr. WYDEN. In the op-ed, we point out that legislators and the public know next to nothing about how the government conducts the searches and that the government itself is planning to use software that has not been properly vetted by outside security experts. A bungled government hack could damage systems at hospitals, the power grid, transportation, or other critical infrastructure, and Congress has not had a single hearing on this issue—not one.

In addition, the Rules Enabling Act gives Congress the opportunity to weigh in, which is exactly what my colleagues hope to be doing now on this important issue.

Because of these serious damages, I introduced a bill called the Stop Mass Hacking Act with a number of my colleagues, including Senators DAINES and PAUL. This bill would stop these changes from taking effect, and I am here this morning to ask unanimous consent that the bill be taken up and passed.

Mr. President, I ask unanimous consent that the Judiciary Committee be discharged from further consideration of S. 2952 and the Senate proceed to its immediate consideration, that the bill be read a third time and passed, and the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Is there objection?

The majority whip.

Mr. CORNYN. Mr. President, reserving the right to object, I respect our colleague's right to come to the floor and ask unanimous consent. I understand that there are three unanimous consent requests, and I will be objecting to all three of them. I will reserve my statement as to why I am objecting after the third request.

At this point, I object to the unanimous consent request.

The PRESIDING OFFICER. Objection is heard.

Mr. WYDEN. Mr. President, I wish to recognize my colleague from Montana, and after my colleague from Montana speaks, my friend from Delaware will address the Senate.

The PRESIDING OFFICER. The Senator from Montana.

Mr. DAINES. Mr. President, I thank my colleague from Oregon, Senator WYDEN, for talking about this important issue on the floor today.

We shop online with our credit cards, order medicine with our electronic health care records, talk to friends, share personal information, Skype, post beliefs and photos on social media, or Snapchat fun moments, all the while believing everything is safe and secure. It is more important now than ever to ensure that the information we store on our devices is kept safe and that our right to privacy is protected, and that is what we are really talking about here today. How can we ensure that our information is both safe and secure from hacking and government surveillance?

Certainly technology has made our lives easier, but it has also made it easier for criminals to commit crimes and evade law enforcement. In short, our laws aren't keeping up with 21st-century technology advances. But the government's solution to this problem we are talking about today, the change to rule 41 of the Federal Rules of Criminal Procedure, represents a major policy shift in the way the government investigates cyber crime. This proposed solution essentially gives the government a blank check to infringe upon our civil liberties. The change greatly expands the hacking power of the Federal Government, allowing the search of potentially millions of Americans' devices with a single warrant. What this means is that the victims of hacks could be hacked again by their very own government.

You would think such a drastic policy change that directly impacts our Fourth Amendment right would need to come before Congress. It would need to have a hearing and be heard before the American people with full transparency. But, in fact, we have had no hearings. There has been no real debate on this issue.

My colleagues and I have introduced bipartisan, bicameral legislation to stop the rule change and ensure that the American people have a voice. The American people deserve transparency, and Congress needs time to review this policy to ensure that the privacy rights of Americans are protected.

The fact that the Department of Justice is insisting this rule change take effect on December 1—that is tonight at midnight—frankly, should send a shiver down the spines of all Americans.

My colleagues and I are here today to not only wake up Americans to this great expansion of powers by our government but also to urge our colleagues to join this bipartisan effort to stop rule 41 changes without duly considering the impact to our civil liberties. Our civil liberties and our Fourth Amendment can be chipped away little by little until we barely recognize them anymore. We simply can't give unlimited power for unlimited hacking which puts Americans' civil liberties at risk.

Again, I thank my colleagues from Delaware and Oregon for joining me here today, and I yield to my friend and colleague from Delaware, Senator COONS.

The PRESIDING OFFICER. The Senator from Delaware.

UNANIMOUS CONSENT REQUEST—S. 3475

Mr. COONS. Mr. President, I thank my colleagues, Senator WYDEN and Senator DAINES. They have worked tirelessly to address this pressing issue of the pending change to privacy protections contained in a proposed change to the Federal Rules of Criminal Procedure.

As you have heard, if Congress fails to act today and thoroughly consider and debate these rule changes, they will go into effect at midnight tonight. They will take effect tomorrow, December 1. I believe it is essential that these rules strike a careful balance, giving law enforcement the tools they need to investigate cyber attacks and cyber crimes to keep us safe while also protecting Americans' constitutional rights to freedom from unreasonable searchs, our right to privacy.

Neither the Senate nor House has held a single hearing or markup to evaluate these changes to the Federal Rules of Criminal Procedure. The body of government closest to the people has utterly failed to weigh in on an issue that can immediately and directly impact our constituents—our citizens. While the proposed changes are not necessarily bad or good, they are serious and present significant privacy concerns that warrant careful consideration and debate.

All Americans should want criminal investigations to proceed quickly and thoroughly, but, as I have said, I am concerned that these changes would remove important judicial safeguards by having one judge decide on a search that would give our government the ability to search and possibly alter thousands of computers owned by innocent and unknowing American citizens all over our country.

Members of Congress should have an opportunity to consider this information seriously. We should carefully evaluate the merits of these proposed changes and their ramifications. I think it is our duty to have a frank and open discussion so we can think about the unintended consequences and protect our constituents' rights. Two weeks ago, I introduced legislation that would give Congress the time to have that conversation. The Review the Rule Act, or S. 3475, would delay the changes to rule 41 until July 1, 2017. That bill is cosponsored by Senators WYDEN, LEAHY, BALDWIN, and FRANKEN, as well as Republican Senators DAINES, LEE, and PAUL. That list of Senators from every part of our ideological spectrum is just a reminder that this is not a partisan issue. This is a bipartisan group of Senators raising questions and challenges to a proposal by the Obama administration's Justice Department.

I think it is important to remind anyone watching or listening that we want to ensure that the American people are kept safe from hackers and online criminal activity. We want law enforcement to have the tools to investigate and address potential threats, but we shouldn't have to sacrifice our rights to privacy and protection from unreasonable searches and seizures just to achieve that protection.

I encourage my colleagues to join me in supporting this legislation and